UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,680	01/21/2004	Osamu Kobayashi	GENSP047	5247

22434 7590 06/23/2008
BEYER WEAVER LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
SHAIFER HARRIMAN, DANT B	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
06/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/762,680	**Applicant(s)** KOBAYASHI, OSAMU	
	Examiner DANT B. SHAIFER HARRIMAN	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on *27 March 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 - 16 & 18 & 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 - 16 & 18 & 20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 January 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *05/09/2008*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

Claims 1, 6, 10, 11, 12, 20 are amended in the instant application.

Claims 2, 8, 9, 13, are original in the instant application.

Claims 3, 4, 5, 7, 14, 15, 16 are previously presented in the instant application.

Claims 17, 19 are cancelled in the instant application.

Response to Arguments

Applicant's arguments filed 3/27/2008 have been fully considered but they are moot on grounds of new rejection. Please see office action below for details.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim(s) 1, 3, 4, 5, 6, 9, 10, 11, 12, 13, 14, 15, 16, 18, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Huuhtanen (Publication # EP 0 674 441 A1) in view of Pasqualino (Publication #2002/0163598 A1) further in view of Kluttz (US Patent No. 6598161 B1).

Huuhtanen discloses:

1. A packet based high bandwidth copy protection method

comprising:

- displaying the decrypted data packets by the sink device(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device that is attached to the signal receiver or sink unit, that will allow the customer to view the displayed decrypted data packets).

6. A system for providing high bandwidth copy protection in a

packet based system, comprising:

- a sink unit coupled to the source unit arranged to receive the data packets from the source unit(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink unit.);

- a decryption unit coupled to the sink unit arranged to appropriately decrypt the encrypted data packets(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink unit.);

- an encryption/decryption values generator arranged to provide the first and at least the second set of encryption/decryption values to the decryption unit(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink unit that will posses the necessary decryption values generator that will arrange for the decrypting of the selected encrypted data packets received by the sink device.); and

- a processor for processing the decrypted data packets for display by the sink unit (Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device that is attached to the signal receiver or sink unit, that will allow the customer to view the displayed decrypted data packets).

12. Computer program product executable by a processor for providing a packet based high bandwidth copy protection, the computer program product comprising:

- computer code for encrypting forming a first group of the data packets by encrypting some of the data packets based upon a first set of encryption values, wherein the number of encrypted data packets in the first group is less than the number of data packets formed at the source device(Col. 3, lines 5 – 9 & Col. 3, lines 47 – 50, the examiner notes that the customers receiver (i.e. cable box) can be considered a computer program product. Based on the fact that a cable box has both a hardware and software components, without hardware or software component, the other will be unable to operate; the cable box contains the necessary software to request and retrieve TV programming (i.e. movies, sporting events etc.) from the operators server (forming a number of data packets at the operators server.), moreover the operator receiver or cable box contains the software necessary to implement the goods and services promised by the operator, which is through the execution of the operators server (which contains the operators multimedia content processor.) The customers receiver will also have the necessary software for encryption/decryption generator for sending encrypted messages (i.e. cable box malfunction indications that facilitates problem solving and better customer service, for example sending multimedia data packets back to the operators server (i.e. if there is a an error in the sending of multimedia content, the receiver will request that a particular data packet be sent back to the receiver in order to complete the multimedia content transmission to the customer and will be encrypted so that a hacker cannot gain information on how to break into a the cable TV system.);

- computer code for displaying the decrypted data packets by the sink device(Col. 3, lines 5-9, the examiner notes that the cable box or the operators cable box will have the necessary software or decryption software or a module that is attached or is in communication with the cable box receiver that allows the decryption of the incoming encrypted data packets, due to the fact the data packets and also encryption key from the operators server will be encrypted, which is needed in order for the display of the decrypted data packets); and

- computer readable medium for storing the computer code(Col. 3, lines 5 – 9 & Col. 3, lines 47 – 50, the examiner notes that the customers receiver(i.e. cable box, which is portable) can be considered a computer program product. Based on the fact that a cable box has both hardware and software components, without the hardware component or software component, the other component will be unable to operate; the cable box contains the necessary software to retrieve TV programming (i.e. movies, sporting events etc.) from the operators server, which is a computer, which is able to communicate and or read the signals from the cable box, initiated by the customer or user commands, the receiver is also able to interpret the operators server commands.).

Huuhtanen does not explicitly disclose:

1. A packet based high bandwidth copy protection method

comprising:

- forming a number of related data packets at a source device();
- forming a first group of encrypted data packets by encrypting some of the data packets based upon a first set of encryption/decryption values, wherein the number of encrypted data packets in the first group of encrypted data packets is less than the number of data packets formed at the source device();
- forming second group of encrypted data packets by encrypting those data packets not already encrypted based upon a second set of encryption values wherein each and every one of the related data packets is encrypted and belongs to either the first or the second group of encrypted data packets(); and

- transmitting the encrypted data packets from the source device to a sink device coupled thereto();

- decrypting the first group of encrypted data packets using the a first set of encryption/decryption values corresponding to the first set of encryption values();

- decrypting the second group of encrypted data packets using the a second set of decryption values corresponding to the at least second set of encryption values_concurrently with the decrypting of the first set of encrypted data packets(); and

3. A method as recited in claim 1, further comprising:

- forming a first control data packet associated with the first set of encryption/decryption values();

- using the first control data packet to identify the first group of encrypted data packets();

- forming a second control data packet associated with the second set of encryption/decryption values(); and

- using the second control data packet to identify the second group of encrypted data packets, wherein the encryption/decryption values include a Vsync control value, an Hsync control value, and a CNTL3 control value().

4. A method as recited in claim 3,

- using the first set of encryption/decryption values included in the first control data packet to decrypt the first group of encrypted data packets and using the second set of encryption/decryption values included in the second control data packet to decrypt the second group of encrypted data packets().

5. A method as recited in claim 4, wherein

- when the CNTL3 control value is active, then the corresponding data packet is encrypted().

6. A system for providing high bandwidth copy protection in a packet based system, comprising:

- a source unit arranged to provide a number of related data packets();

- an encryption unit coupled to the source unit arranged to encrypt selected ones of the data packets sent from the source unit to the sink unit using a first set of encryption values and the remaining data packets using at least a second set of encryption values different from the first set of encryption values wherein each and every one of the data packets is encrypted();

9. A system as recited in claim 8, wherein

- the display unit includes a number of speakers arranged to transmit audio signals based upon processed ones of the audio data packets().

10. A system as recited in claim 9, wherein

- the encryption/decryption values include a Vsync control signal, a Hsync control signal corresponding to the video data packets().

11. A system as recited in claim 10, wherein

- the encryption/decryption values further includes a CNTL3 control value to flag those data packets that are encrypted().

12. Computer program product executable by a processor for providing a packet based high bandwidth copy protection, the computer program product comprising:

- computer code for forming a number of related data packets at a source device;

- computer code for forming a second group of encrypted data packets by encrypting those data packets not already encrypted based upon a second set of encryption values wherein each and every one of the related data packets is encrypted and belongs to either the first or the second group of encrypted data packets();

- computer code for transmitting the encrypted data packets from the source device to a sink device coupled thereto();
- computer code for decrvpting the first group of encrypted data packets using a first set of decrvption values corresponding to the first set of encrvption values();
- computer code for decrvpting the second group of encrypted data packets using a second set of decrvption values corresponding to the at least second set of encrvption values concurrentlv with the decrvpting of the first set of encrypted data packets();

13. Computer program product as recited in claim 12, wherein

- the source device is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets().

14. Computer program product as recited in claim 13, wherein

- the encryption control values include a Vsync control value, an Hsync control value, and a CNTL3 control value().

15. Computer program product as recited in claim 14, wherein

- each of the data packets is associated with a specific CNTL3 control value().

16. Computer program product as recited in claim 15, wherein

- when the CNTL3 control value is active, then the corresponding data packet is encrypted().

18. A method as recited in claim 1, wherein

- the first set of encryption values is different than the second set of encryption values().

20. A method as recited in claim 1,

- using the encryption/decryption values included in the first control data packet to decrypt the first group of encrypted data packets and using the encryption/decryption values included in the second control data packet to decrypt at least the second group of encrypted data packets().

However, Pasqualino discloses:

3. A method as recited in claim 1, further comprising:

- using the second control data packet to identify the second group of encrypted data packets, wherein the encryption/decryption values include a Vsync control value, an Hsync control value, and a CNTL3 control value (Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3).

5. A method as recited in claim 4, wherein

- when the CNTL3 control value is active, then the corresponding data packet is encrypted(Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3).

9. A system as recited in claim 8, wherein

- the display unit includes a number of speakers arranged to transmit audio signals based upon processed ones of the audio data packets(Paragraphs: 0047& 0065, Examiner notes, DVAA enables Pasqualino to teach a display unit that has speakers because it is the representative of the standard for use in the consumer industry for transmitting high quality, multi-channel audio and auxiliary data over a digital video link).

10. A system as recited in claim 9, wherein

- the encryption/decryption values include a Vsync control signal, a Hsync control signal corresponding to the video data packets(Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3).

11. A system as recited in claim 10, wherein

- the encryption/decryption values further includes a CNTL3 control value to flag those data packets that are encrypted(Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3).

13. Computer program product as recited in claim 12, wherein

- the source device is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets(Paragraph: 0047, 0051).

14. Computer program product as recited in claim 13, wherein

- the encryption control values include a Vsync control value, an Hsync control value, and a CNTL3 control value(Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3).

15. Computer program product as recited in claim 14, wherein

- each of the data packets is associated with a specific CNTL3 control value(Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3).

16. Computer program product as recited in claim 15, wherein

- when the CNTL3 control value is active, then the corresponding data packet is encrypted(Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3).

20. A method as recited in claim 1,

- using the encryption/decryption values included in the first control data packet to decrypt the first group of encrypted data packets and using the encryption/decryption values included in the second control data packet to decrypt at least the second group of encrypted data packets(Paragraphs: 82, 93, 95, 97, 98, figure 2 & 3).

Further, Kluttz discloses:

1. A packet based high bandwidth copy protection method

comprising:

- forming a number of related data packets at a source device(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 – 6, the examiner notes that the examiner interprets “related," to mean that the media being encrypted is all the same media, for example, a video clip that contains audio and video data packets is being encrypted and not a video/audio clip and an unrelated text document is being encrypted together);
- forming a first group of encrypted data packets by encrypting some of the data packets based upon a first set of encryption/decryption values, wherein the number of encrypted data packets in the first group of encrypted data packets is less than the number of data packets formed at the source device(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60,

Col. 7, lines 3 - 6);

- forming second group of encrypted data packets by encrypting those data packets not already encrypted based upon a second set of encryption values wherein each and every one of the related data packets is encrypted and belongs to either the first or the second group of encrypted data packets(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 - 6); and

- transmitting the encrypted data packets from the source device to a sink device coupled thereto(col. 7, lines 28 - 45);

- decrypting the first group of encrypted data packets using the a first set of encryption/decryption values corresponding to the first set of encryption values(Col. 2, lines 21 – 28, Col. 2, lines 33 – 40, Col. 2, lines 49 – 52, col. 6, lines 28 – 31);

- decrypting the second group of encrypted data packets using the a second set of decryption values corresponding to the at least second set of encryption values concurrently with the decrypting of the first set of encrypted data packets(Col. 2, lines 21 – 28, Col. 2, lines 33 – 40, Col. 2, lines 49 – 52, col. 6, lines 28 – 31); and

3. A method as recited in claim 1, further comprising:

- forming a first control data packet associated with the first set of encryption/decryption values(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 – 6,);

- using the first control data packet to identify the first group of encrypted data packets(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 – 6,);

- forming a second control data packet associated with the second set of encryption/decryption values(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 – 6,); and

4. A method as recited in claim 3,

- using the first set of encryption/decryption values included in the first control data packet to decrypt the first group of encrypted data packets and using the second set of encryption/decryption values included in the second control data packet to decrypt the second group of encrypted data packets(Col. 2, lines 21 – 28, Col. 2, lines 33 – 40, Col. 2, lines 49 – 52, col. 6, lines 28 – 31).

6. A system for providing high bandwidth copy protection in a packet based system, comprising:

- a source unit arranged to provide a number of related data packets(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 – 6, the examiner notes that the examiner interprets “related," to mean that the media being encrypted is all the same media, for example, a video clip that contains audio and video data packets is being encrypted and not a video/audio clip and an unrelated text document is being encrypted together);

- an encryption unit coupled to the source unit arranged to encrypt selected ones of the data packets sent from the source unit to the sink unit using a first set of encryption values and the remaining data packets using at least a second set of encryption values different from the first set of encryption values wherein each and every one of the data packets is encrypted(Col. 2, lines 33 – 40 & Col. 7, lines 7 - 16);

12. Computer program product executable by a processor for providing a packet based high bandwidth copy protection, the computer program product comprising:

- computer code for forming a number of related data packets at a source device (Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 – 6, the examiner notes that the examiner interprets “related," to mean that the media being encrypted is all the same media, for example, a video clip that contains audio and video data packets is being encrypted and not a video/audio clip and an unrelated text document is being encrypted together);

- computer code for forming a second group of encrypted data packets by encrypting those data packets not already encrypted based upon a second set of encryption values wherein each and every one of the related data packets is encrypted and belongs to either the first or the second group of encrypted data packets(Col. 3, lines 63 – 67 & Col. 4, lines 1 – 28, & Col. 5, lines 30 - 55);

- computer code for transmitting the encrypted data packets from the source device to a sink device coupled thereto(Col. 3, lines 63 – 67 & Col. 4, lines 1 – 28, & Col. 5, lines 30 - 55);
- computer code for decrvpting the first group of encrypted data packets using a first set of decrvption values corresponding to the first set of encrvption values(Col. 3, lines 63 – 67 & Col. 4, lines 1 – 28, & Col. 5, lines 30 - 55);
- computer code for decrvpting the second group of encrypted data packets using a second set of decrvption values corresponding to the at least second set of encrvption values concurrentlv with the decrvpting of the first set of encrypted data packets(Col. 3, lines 63 – 67 & Col. 4, lines 1 – 28, & Col. 5, lines 30 - 55);

18. A method as recited in claim 1, wherein

- the first set of encryption values is different than the second set of encryption values(Col. 2, lines 32 - 40).

Huuhtanen and Pasqualino and Kluttz are analogous art because they are from the “same field of endeavor,” which is the field of encryption of information being passed from a source to a sink device.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Huuhtanen and Pasqualino and Kluttz before him or her, to modifying claim 1 & 6 & 12, 13, Huuhtanen teaches the scrambling an entire digital signal or digital content by encrypting with one encryption key that is being sent from a source to a sink device, which does not meet the claim limitations of claim 1, however to one of ordinary skill in the art would find the combination of Kluttz with Huuhtanen by allowing the information or content to encrypted by specific portions of the data, by the use of different encryption/decryption keys, and allowing access to only specific levels of multimedia (i.e. text document, audio/video clip, graphics.... etc), when the multimedia content is being sent from a source to a sink device, and also the computer program implementation of the above combination.

Referring to claim 3, 4, 5, 10, 11, 14, 15, 16, 20, Huuhtanen only teaches encryption of data packets of a digital signal, the encryption of the data packets do not teach the encryption/decryption values include a Vsync control signal, a Hsync control signal corresponding to the video data packets or the encryption/decryption values further includes a CNTL3 control value to flag those data packets that are encrypted or using the encryption/decryption values included in the first control data packet to decrypt the first group of encrypted data packets and using the encryption/decryption values included in the second control data packet to decrypt at least the second group of encrypted data packets, however to one or ordinary skill in the art, the combination of Huuhtanen and Pasqualino would render the above claims obvious, thus Pasqualino teaches, the control values/signals (CNTL3) associated with the transmission of data packets (i.e. identify which data packets are encrypted), because by selecting only some of the plurality of data packets to be encrypted and associating a specific control packet and encryption/decryption values will allow the receiver to identify the incoming data packets that are encrypted and unencrypted. This protocol will also make it very hard to obtain an illegal signal from the cable service operator, due to the fact that each successive grouping of data packet has different encryption/decryption values and control packet.

Referring to claim 18, Huuhtanen teaches the scrambling an entire digital signal or digital content by encrypting with one encryption key that is being sent from a source to a sink device, which does not meet the claim limitations of claim 18, however to one of ordinary skill in the art would find the combination of Kluttz with Huuhtanen by allowing the information or content to encrypted by specific portions of the data, by the use of different encryption/decryption keys, and allowing access to only specific levels of multimedia (i.e. text document, audio/video clip, graphics.... etc), when the multimedia content is being sent from a source to a sink device, and also the computer program implementation of the above combination.

The suggestion/motivation for doing so would have been to prevent non-paying or non-subscribing customers from obtaining or pirating free service (Pasqualino: Paragraph: 0053) and preventing the pirating of all video and audio stream content or data packets being transferred from a source (TV operators equipment) to a sink (customers cable TV box) in a lossless digital domain. (Pasqualino: Paragraph: 49), by allowing only a user access to specific levels of a multimedia, in Col. 1, lines 20 -

26 of Kluttz also please see **KSR** v. **Teleflex**, 127 S.Ct. 1727, 1740, 82 USPQ2d 1385, 1396 (2007).

Claim(s) 2, 7, 8 are rejected under 35 USC 103 (a) as being obvious over Huuhtanen (Publication # EP 0 674 441 A1) in view of Kluttz (US Patent No. 6598161 B1) further in view of Faber (Pat. # 6477252 B1)

Huuhtanen discloses:

1. A packet based high bandwidth copy protection method

comprising:

- displaying the decrypted data packets by the sink device(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device that is attached to the signal receiver or sink unit, that will allow the customer to view the displayed decrypted data packets).

6. A system for providing high bandwidth copy protection in a

packet based system, comprising:

- a sink unit coupled to the source unit arranged to receive the data packets from the source unit(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink unit.);

- a decryption unit coupled to the sink unit arranged to appropriately decrypt the encrypted data packets(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink unit.);
- an encryption/decryption values generator arranged to provide the first and at least the second set of encryption/decryption values to the decryption unit(Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device attached the signal receiver or sink unit that will posses the necessary decryption values generator that will arrange for the decrypting of the selected encrypted data packets received by the sink device.); and
- a processor for processing the decrypted data packets for display by the sink unit (Col 3, lines 5 –10, the examiner notes that the customer has a descrambling device that is attached to the signal receiver or sink unit, that will allow the customer to view the displayed decrypted data packets).

Huuhtanen does not explicitly disclose:

1. A packet based high bandwidth copy protection method

comprising:

- forming a number of related data packets at a source device();

- forming a first group of encrypted data packets by encrypting some of the data packets based upon a first set of encryption/decryption values, wherein the number of encrypted data packets in the first group of encrypted data packets is less than the number of data packets formed at the source device();

- forming second group of encrypted data packets by encrypting those data packets not already encrypted based upon a second set of encryption values wherein each and every one of the related data packets is encrypted and belongs to either the first or the second group of encrypted data packets(); and

- transmitting the encrypted data packets from the source device to a sink device coupled thereto();

- decrypting the first group of encrypted data packets using t-he a first set of encryption/decryption values corresponding to the first set of encryption values();

- decrypting the second group of encrypted data packets using the a second set of decryption values corresponding to the at least second set of encryption values_concurrently with the decrypting of the first set of encrypted data packets(); and

2. A method as recited in claim 1, wherein

- the source device is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets().

6. A system for providing high bandwidth copy protection in a packet based system, comprising:

- a source unit arranged to provide a number of related data packets();

- an encryption unit coupled to the source unit arranged to encrypt selected ones of the data packets sent from the source unit to the sink unit using a first set of encryption values and the remaining data packets using at least a second set of encryption values different from the first set of encryption values wherein each and every one of the data packets is encrypted();

7. A system as recited in claim 6, wherein

- the source unit is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets().

8. A system as recited in claim 7, wherein

- the sink unit is a display unit arranged to display processed ones of the video data packets().

However, Kluttz discloses:

1. A packet based high bandwidth copy protection method

comprising:

- forming a number of related data packets at a source device(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 – 6, the examiner notes that the examiner interprets “related," to mean that the media being encrypted is all the same media, for example, a video clip that contains audio and video data packets is being encrypted and not a video/audio clip and an unrelated text document is being encrypted together);

- forming a first group of encrypted data packets by encrypting some of the data packets based upon a first set of encryption/decryption values, wherein the number of encrypted data packets in the first group of encrypted data packets is less than the number of data packets formed at the source device(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 - 6);

- forming second group of encrypted data packets by encrypting those data packets not already encrypted based upon a second set of encryption values wherein each and every one of the related data packets is encrypted and belongs to either the first or the second group of encrypted data packets(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 - 6); and

- transmitting the encrypted data packets from the source device to a sink device coupled thereto(col. 7, lines 28 - 45);

- decrypting the first group of encrypted data packets using the a first set of encryption/decryption values corresponding to the first set of encryption values(Col. 2, lines 21 – 28, Col. 2, lines 33 – 40, Col. 2, lines 49 – 52, col. 6, lines 28 – 31);

- decrypting the second group of encrypted data packets using the a second set of decryption values corresponding to the at least second set of encryption values concurrently with the decrypting of the first set of encrypted data packets(Col. 2, lines 21 – 28, Col. 2, lines 33 – 40, Col. 2, lines 49 – 52, col. 6, lines 28 – 31); and

6. A system for providing high bandwidth copy protection in a packet based system, comprising:

- a source unit arranged to provide a number of related data packets(Col. 2, lines 5 – 15, Col. 6, lines 55 – 60, Col. 7, lines 3 – 6, the examiner notes that the examiner interprets “related," to mean that the media being encrypted is all the same media, for example, a video clip that contains audio and video data packets is being encrypted and not a video/audio clip and an unrelated text document is being encrypted together);

- an encryption unit coupled to the source unit arranged to encrypt selected ones of the data packets sent from the source unit to the sink unit using a first set of encryption values and the remaining data packets using at least a second set of encryption values different from the first set of encryption values wherein each and every one of the data packets is encrypted(Col. 2, lines 33 – 40 & Col. 7, lines 7 - 16);

Further, Faber discloses:

2. A method as recited in claim 1, wherein

- the source device is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets(Column 1, lines 47 through 55).

7. A system as recited in claim 6, wherein

- the source unit is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets (Column 1, lines 48 –50, a video source device provides a basis value to a symmetric ciphering/deciphering process to a video sink device, to which the video source device is to provide video content).

8. A system as recited in claim 7, wherein

- the sink unit is a display unit arranged to display processed ones of the video data packets(Column 1, lines 51 –54), the video source device ciphers the video content for transmission to the video sink device, including generation of a first cipher key through functional transformation of the basis value).

Huuhtanen and Kluttz and Faber are analogous art because they "same field of endeavor," which is the field of encryption of information being passed from a source to a sink device.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Huuhtanen and Kluttz and Faber before him or her, referring to claims 2 & 7, Huuhtanen doesn't teach a video source and video sink wherein the number of data packets include some audio data packets and some video data packets, thus it would be obvious of one of ordinary skill in the art, to combine Huuhtanen with Faber to include a a video source device provides a basis value to a symmetric ciphering/deciphering process to a video sink device, to which the video source device is to provide video content.

Referring to claim 8, Huuhtanen doesn't teach a sink unit that displays processed ones of video data packets, however thus it would be obvious of one of ordinary skill in the art, to combine Huuhtanen with Faber to include a sink unit display unit arranged to display processed ones of the video data packets.

The suggestion/motivation for doing so would have been to allow only a user access to specific levels of a multimedia, in Col. 1, lines 20 - 26 of Kluttz, also Col. 2, lines 35 – 48 of Faber also please see **KSR** v. **Teleflex**, 127 S.Ct. 1727, 1740, 82 USPQ2d 1385, 1396 (2007).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANT B. SHAIFER HARRIMAN whose telephone number is (571)272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DSH

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134